


# Exhibit 2

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

Claim Language	Where in the Accused Product(s) Each Limitation of the Asserted Claim(s) are Found
<p><b>Claim 10.</b> A method of creating and maintaining a dynamic decoy system based on a protected system comprising:</p>	<p>Defendant Trend Micro’s accused methods embody creating and maintaining a dynamic decoy system based on a protected system, as claimed in claim 10 of the ‘698 patent. Trend Micro controls its accused methods for its benefit (<i>e.g.</i>, fiscal gains). Trend Micro’s methods also benefits end-users of the method (<i>e.g.</i>, security and protection).</p> <p>For example, Trend Micro’s suite of Deep Discovery products (<i>e.g.</i>, the Deep Discovery Analyzer; Deep Discovery Inspector; Deep Discovery Director; etc.) create and maintain a dynamic decoy system (<i>e.g.</i> sandboxes) based on a protected system (<i>e.g.</i> a CPU; application; device; etc.).</p> <div data-bbox="545 873 1494 1058" style="border: 1px solid black; padding: 5px;">  <p><b>Custom Sandbox Analysis</b> uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&amp;C), and more, as well as supporting manual or automated file and URL submission.</p> </div> <p>Source: “Deep Discovery Analyzer,”  <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html</a>.</p> <div data-bbox="545 1146 1474 1606" style="border: 1px solid black; padding: 5px;"> <p>“Trend Micro™ Deep Discovery™ Inspector is a physical or virtual network appliance that monitors 360 degrees of your network to create complete visibility into all aspects of targeted attacks, advanced threats, and ransomware. <b><u>By using specialized detection engines and custom sandbox analysis, Deep Discovery Inspector identifies advanced and unknown malware, ransomware, zero-day exploits, command and control (C&amp;C) communications, and evasive attacker activities that are invisible to standard security defenses.</u></b> Detection is enhanced by monitoring all physical, virtual, north-south, and east-west traffic.”</p> <p>Source: <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/inspector.html</a> (emphasis added)</p> </div>

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

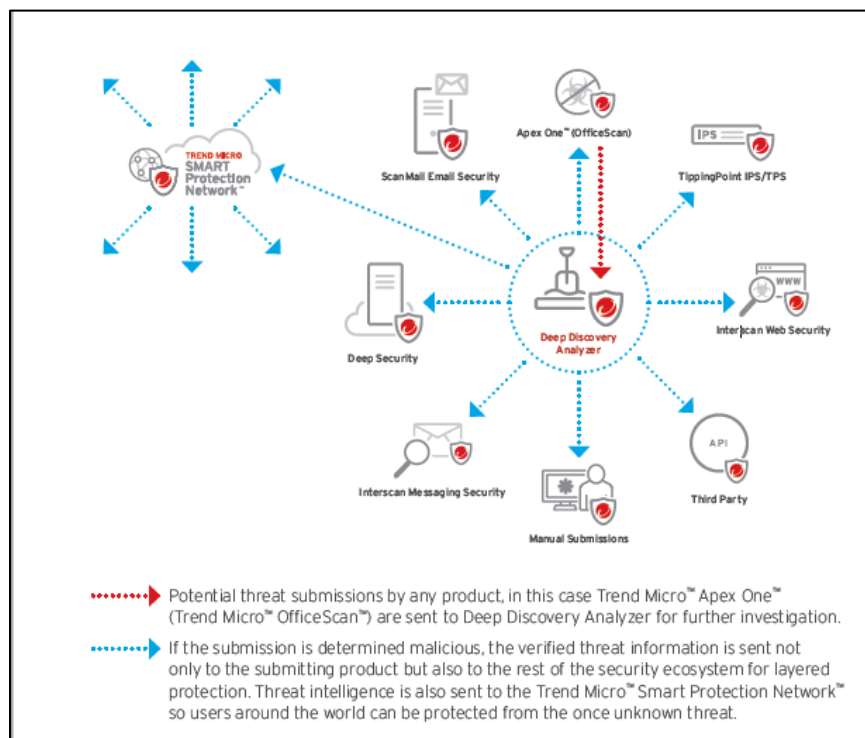
Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

“Deep Discovery Analyzer extends the value of existing security investments from Trend Micro and third parties (through a web services API) by providing **custom sandboxing and advanced analysis**. It can also provide expanded sandboxing capabilities to other Trend Micro products. **Suspicious objects can be sent to the Analyzer sandbox for advanced analysis using multiple detection methods.** If a threat is discovered, security solutions can be updated automatically.”

Source: “Deep Discovery Analyzer” Datasheet,  
[https://www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html](https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html)  
 (emphasis added)

As shown in the diagram below, “potential threat submissions” are sent to the Deep Discovery Analyzer. If such a submission is determined to be malicious, the entire Trend Micro Security Ecosystem and Smart Protection Network is updated for all users.






Source: “Layered Security for Detection and Response” brief,  
[www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f](https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f)

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

	<p>Depending on the result of the pre-scan, Deep Discovery Analyzer performs the following actions.</p> <table border="1"> <thead> <tr> <th>RESULT</th><th>ACTION</th></tr> </thead> <tbody> <tr> <td>If the sample is a known good file / URL</td><td> <ul style="list-style-type: none"> <li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li> </ul> </td></tr> <tr> <td>If the sample does not match any existing record</td><td> <ul style="list-style-type: none"> <li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li> <li>Deep Discovery Analyzer treats the sample as a submission and sends it to the Submission queue. The sample is not shown on the <b>ICAP Pre-scan</b> tab.</li> <li>Deep Discovery Analyzer adds the sample to the Deep Discovery Analyzer database to benefit later submissions.</li> </ul> <hr/> <p> <b>Note</b></p> <p>If Virtual Analyzer does not support the file type of a submitted sample, Deep Discovery Analyzer does not send the sample to the Submission queue or add to the Deep Discovery Analyzer database.</p> <hr/> </td></tr> <tr> <td>If the sample matches a known malicious threat</td><td> <ul style="list-style-type: none"> <li>Deep Discovery Analyzer responds with a <code>403 Forbidden</code> message to the ICAP client.</li> <li>Deep Discovery Analyzer logs the sample and displays sample details on the <b>ICAP Pre-scan</b> tab.</li> </ul> </td></tr> </tbody> </table> <p>Source: “Submissions,” <a href="https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf">https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf</a> at Chapter 4, page 11</p>	RESULT	ACTION	If the sample is a known good file / URL	<ul style="list-style-type: none"> <li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li> </ul>	If the sample does not match any existing record	<ul style="list-style-type: none"> <li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li> <li>Deep Discovery Analyzer treats the sample as a submission and sends it to the Submission queue. The sample is not shown on the <b>ICAP Pre-scan</b> tab.</li> <li>Deep Discovery Analyzer adds the sample to the Deep Discovery Analyzer database to benefit later submissions.</li> </ul> <hr/> <p> <b>Note</b></p> <p>If Virtual Analyzer does not support the file type of a submitted sample, Deep Discovery Analyzer does not send the sample to the Submission queue or add to the Deep Discovery Analyzer database.</p> <hr/>	If the sample matches a known malicious threat	<ul style="list-style-type: none"> <li>Deep Discovery Analyzer responds with a <code>403 Forbidden</code> message to the ICAP client.</li> <li>Deep Discovery Analyzer logs the sample and displays sample details on the <b>ICAP Pre-scan</b> tab.</li> </ul>
RESULT	ACTION								
If the sample is a known good file / URL	<ul style="list-style-type: none"> <li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li> </ul>								
If the sample does not match any existing record	<ul style="list-style-type: none"> <li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li> <li>Deep Discovery Analyzer treats the sample as a submission and sends it to the Submission queue. The sample is not shown on the <b>ICAP Pre-scan</b> tab.</li> <li>Deep Discovery Analyzer adds the sample to the Deep Discovery Analyzer database to benefit later submissions.</li> </ul> <hr/> <p> <b>Note</b></p> <p>If Virtual Analyzer does not support the file type of a submitted sample, Deep Discovery Analyzer does not send the sample to the Submission queue or add to the Deep Discovery Analyzer database.</p> <hr/>								
If the sample matches a known malicious threat	<ul style="list-style-type: none"> <li>Deep Discovery Analyzer responds with a <code>403 Forbidden</code> message to the ICAP client.</li> <li>Deep Discovery Analyzer logs the sample and displays sample details on the <b>ICAP Pre-scan</b> tab.</li> </ul>								

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

## Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation
- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC files that can be used in investigations.

It works in conjunction with Threat Connect, the Trend Micro service that correlates suspicious objects detected in your environment and threat data from the Smart Protection Network.

Source: “Virtual Analyzer,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 4, page 2

## DEEP DISCOVERY ANALYZER APPLIANCE SPECIFICATIONS

	Deep Discovery Analyzer
Capacity	38,000 samples/day
Supported File Types	.bat, .cmd, .cell, .chm, .csv, .class, .cls, .dll, .doc, .dot, .docx, .dotx, .docm, .dotm, .cpl, .exe, .sys, .crt, .scr, .qul, .hta, .htm, .html, .hwp, .hwpk, .iqy, .jar, .js, .jse, .jtd, .lnk, .mov, .pdf, .ppt, .pps, .pptx, .ppsx, .psl, .pub, .rtf, .slk, .svg, .swf, .vbe, .vbs, .wsf, .xls, .xla, .xlt, .xlm, .xlsx, .xlsx, .xltx, .xlsm, .xlam, .xltn, .xml, .xht, .xhtml, .url
Supported Operating Systems	Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2003, 2008, 2012, 2016 Mac OS
Form Factor	2U rack-mount, 48.26 cm (19")
Weight	31.5 kg (69.45 lbs)
Dimensions	Width 48.2 cm (18.98") x Depth 75.58 cm (29.75") x Height 8.73 cm (3.44")
Management Ports	10/100/1000 base-T RJ45 port x 1
Data Ports	10/100/1000 base-T RJ45 x 3
AC Input Voltage	100 to 240 VAC
AC Input Current	10A to 5A
Hard Drives	2 x 4 TB 3.5 inch SATA
RAID Configuration	RAID 1
Power Supply	750W redundant
Power Consumption (Max.)	847W (max.)
Heat	2891 BTU/hr. (max.)
Frequency	50/60 HZ
Operating Temp.	50-95 °F (10 to 35 °C)
Hardware Warranty	3 years

Source: “Deep Discovery Analyzer” Datasheet, [https://www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html](https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html) (emphasis added)

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001



Note: Statements made herein are illustrative and not exhaustive

	<p>On information and belief, reasonable discovery will confirm that Trend Micro provides a method for creating and maintaining a dynamic decoy system based on a protected system, as set forth in claim 10 of the ‘698 patent.</p>
<p>creating a dynamic decoy system that substantially parallels relevant portions of a protected system;</p>	<p>Trend Micro’s accused method embodies creating a dynamic decoy system that substantially parallels relevant portions of a protected system. Reasonable discovery will confirm this interpretation.</p> <p>For example, Trend Micro’s Deep Discovery Analyzer gathers potential threats from multiple sources in order to determine malicious content. If the potential threat is considered dangerous it updates the system and sends to the entire security ecosystem. The custom sandbox (<i>e.g.</i>, dynamic decoy system) matches the specific system specification (<i>e.g.</i>, protected system) in order to detect the threats, thereby creating a dynamic decoy system that substantially parallels relevant portions of a protected system.</p> <div data-bbox="540 976 1396 1780" data-label="Diagram"> <p>The diagram illustrates a central 'Deep Discovery Analyzer' (represented by a shield icon) connected to several Trend Micro products: 'Apex One (OfficeScan)', 'ScanMail Email Security', 'IPS', 'TippingPoint IPS/TPS', 'InterScan Web Security', 'API', 'Third Party', 'Manual Submissions', 'InterScan Messaging Security', and 'Deep Security'. A 'Trend Micro SMART Protection Network' is also shown on the left. Red dotted arrows indicate 'Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation.' Blue dotted arrows indicate 'If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat.'</p> </div> <p>Source: “Layered Security for Detection and Response” brief,  <a href="http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f">www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f</a></p>

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

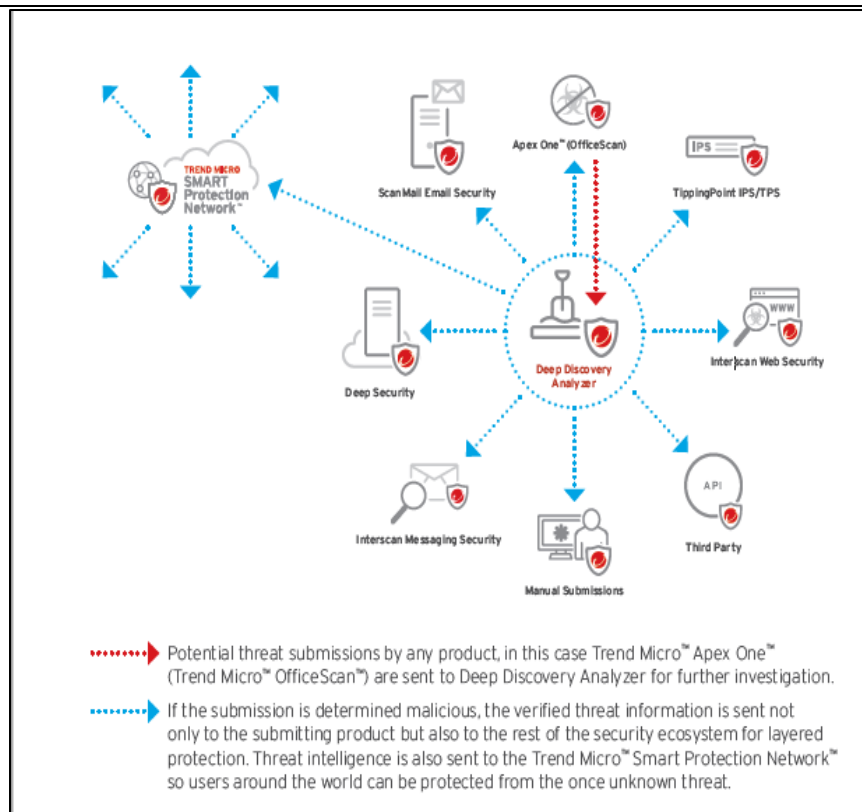
Note: Statements made herein are illustrative and not exhaustive

	<p>Trend Micro’s Custom Sandbox Analysis (<i>e.g.</i>, dynamic decoy machine) uses “virtual images” that “precisely match [a user’s] system configurations, drivers, installed applications, and language versions” (<i>e.g.</i>, relevant portions of a protected system).</p> <div data-bbox="548 541 1490 730">  <p><b>Custom Sandbox Analysis</b> uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&amp;C), and more, as well as supporting manual or automated file and URL submission.</p> </div> <p>Source: “Deep Discovery Analyzer,”  <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html</a>.</p> <div data-bbox="548 804 971 1108"> <p><b>Key Benefits</b></p>  <p><b>Better Detection</b></p> <ul style="list-style-type: none"> <li>• Superior detection versus generic virtual environments.</li> <li>• Superior evasion resistance.</li> </ul> </div> <p>Source: “Deep Discovery Analyzer,”  <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html</a>.</p>
<p>updating the dynamic decoy system based on changes to the protected system;</p>	<p>Trend Micro’s accused methods embody updating the dynamic decoy system based on changes to the protected system. Reasonable discovery will confirm this interpretation.</p> <p>For example, as stated above, Trend Micro’s Deep Discovery Analyzer gathers potential threats from multiple sources in order to determine malicious content. If the potential threat (<i>e.g.</i>, changes to the protected system) is considered dangerous it updates the system and sends to the entire security ecosystem. The custom sandbox (<i>e.g.</i>, dynamic decoy system) matches the specific system specification (<i>e.g.</i>, protected system) in order to detect the threats.</p>

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive



Source: “Layered Security for Detection and Response” brief,

[www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f](http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f)

**Custom Sandbox Analysis** uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Source: “Deep Discovery Analyzer,”

[https://www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html](https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html).




U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

Depending on the result of the pre-scan, Deep Discovery Analyzer performs the following actions.


RESULT	ACTION
If the sample is a known good file / URL	<ul style="list-style-type: none"><li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li></ul>
If the sample does not match any existing record	<ul style="list-style-type: none"><li>Deep Discovery Analyzer sends the original request as a response back to the ICAP client.</li><li>Deep Discovery Analyzer treats the sample as a submission and sends it to the Submission queue. The sample is not shown on the <b>ICAP Pre-scan</b> tab.</li><li>Deep Discovery Analyzer adds the sample to the Deep Discovery Analyzer database to benefit later submissions.</li></ul> <hr/> <div> <b>Note</b> If Virtual Analyzer does not support the file type of a submitted sample, Deep Discovery Analyzer does not send the sample to the Submission queue or add to the Deep Discovery Analyzer database.</div> <hr/>
If the sample matches a known malicious threat	<ul style="list-style-type: none"><li>Deep Discovery Analyzer responds with a <code>403 Forbidden</code> message to the ICAP client.</li><li>Deep Discovery Analyzer logs the sample and displays sample details on the <b>ICAP Pre-scan</b> tab.</li></ul>

Source: “Submissions,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 4, page 11

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

	<p>For further example, and on information and belief, Trend Micro’s Deep Discovery Analyzer monitors the host OS (<i>e.g.</i>, a protected system) and updates the Smart Protection Network, which in turn updates and improves Trend Micro’s sandboxes (<i>e.g.</i>, dynamic decoy system) to protect against new threats.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p><b>Smart Feedback Tab</b></p> <p>Deep Discovery Analyzer integrates the new Trend Micro Feedback Engine. This engine sends threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new threats. Participation in Smart Feedback authorizes Trend Micro to collect certain information from your network, which is kept in strict confidence.</p> <p>Information collected by Smart Feedback:</p> <ul style="list-style-type: none"> <li>• Product ID and version</li> <li>• URLs suspected to be fraudulent or possible sources of threats</li> <li>• Metadata of detected files (file type, file size, SHA-1 hash value, and SHA-1 hash value of parent file)</li> <li>• Detection logs (from Advanced Threat Scan Engine, Predictive Machine Learning engine, and Virtual Analyzer)</li> <li>• Sample of the following detected file types: bat, class, cmd, dll, exe, htm, html, jar, js, lnk, macho, mov, ps1, svg, swf, url, vbe, vbs, wsf</li> <li>• Macros in Microsoft Office files</li> </ul> <p>Source: “Smart Feedback Tab,” <a href="https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf">https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf</a> at Chapter 4, page 75</p> </div>
<p>receiving one or more portions of code;</p>	<p>Trend Micro’s accused methods embody receiving one or more portions of code. Reasonable discovery will confirm this interpretation.</p> <p>For example, portions of code (<i>e.g.</i> files, documents, URLs, etc.) are received in the Deep Discovery Analyzer’s sandbox.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;">  <p><b>Advanced Detection Methods</b> such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly. Analyzer also detects multi-stage malicious files, outbound connections, and repeated C&amp;C from suspicious files.</p> <ul style="list-style-type: none"> <li>• <b>Broad file analysis range</b> examines a wide range of Windows executables, Microsoft® Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing. Custom policies can be defined by file type.</li> <li>• <b>Document exploit detection</b> discovers malware and exploits delivered in common document formats by using specialized detection and sandboxing.</li> <li>• <b>URL analysis</b> Performs sandbox analysis of URLs contained in emails or manually submitted samples.</li> <li>• <b>Web services API and manual submission</b> enables any product or malware analyst to submit suspicious samples. Shares new indicators of compromise (IoC) detection intelligence automatically with Trend Micro and third-party products.</li> <li>• Support for Windows, Mac, and Android™ operating systems.</li> </ul> </div> <p>Source: “Deep Discovery Analyzer” Datasheet, <a href="http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab">www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab</a></p>












U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

### Threat Types

This widget shows the type, amount, and risk level of threats detected in all submissions during the specified time period.

Threat Types				
Period: Last 24 hours		Last refresh: 22/09/2018 14:10:17		
Threat Type	High Risk	Medium Risk	Low Risk	Total
 Ransomware	4	0	0	4
 Coin Miner	0	0	0	0
 Dropper	62	0	117	179
 Worm	35	0	0	35
 Backdoor	28	0	69	97
 Bot	13	0	0	13
 Keylogger	5	0	0	5
 Downloader	3	0	0	3
 File Infector	0	0	0	0
 Exploit	0	0	0	0
 Rootkit	0	0	0	0

The default period is Last 24 hours. Change the period according to your preference.

Click a number under **High Risk**, **Medium Risk**, **Low Risk**, or **Total** to go to the **Submissions** screen and view detailed information.

Source: “Threat Types,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 3, page 9

### Smart Feedback Tab

Deep Discovery Analyzer integrates the new Trend Micro Feedback Engine. This engine sends threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new threats. Participation in Smart Feedback authorizes Trend Micro to collect certain information from your network, which is kept in strict confidence.

Information collected by Smart Feedback:

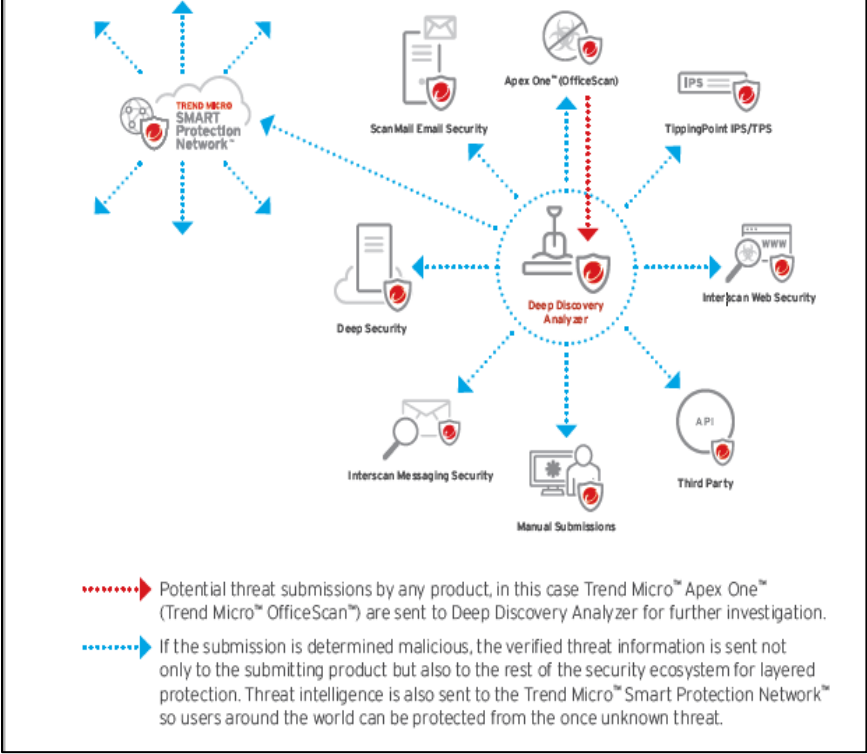
- Product ID and version
- URLs suspected to be fraudulent or possible sources of threats
- Metadata of detected files (file type, file size, SHA-1 hash value, and SHA-1 hash value of parent file)
- Detection logs (from Advanced Threat Scan Engine, Predictive Machine Learning engine, and Virtual Analyzer)
- Sample of the following detected file types: bat, class, cmd, dll, exe, htm, html, jar, js, lnk, macho, mov, ps1, svg, swf, url, vbe, vbs, wsf
- Macros in Microsoft Office files

Source: “Smart Feedback Tab,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 4, page 75

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

	 <p>.....▶ Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation.</p> <p>.....▶ If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat.</p>
<p>introducing the one or more portions of code to the dynamic decoy system;</p>	<p>Trend Micro’s accused methods embody introducing the one or more portions of code to the dynamic decoy system. Reasonable discovery will confirm this interpretation.</p> <p>For example, one or more portions of code (<i>e.g.</i> files, documents, URLs, etc.) are introduced to the dynamic decoy system (<i>e.g.</i>, Deep Discovery Analyzer’s sandbox).</p>

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive



**Advanced Detection Methods** such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly. Analyzer also detects multi-stage malicious files, outbound connections, and repeated C&C from suspicious files.

- **Broad file analysis range** examines a wide range of Windows executables, Microsoft® Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing. Custom policies can be defined by file type.
- **Document exploit detection** discovers malware and exploits delivered in common document formats by using specialized detection and sandboxing.
- **URL analysis** Performs sandbox analysis of URLs contained in emails or manually submitted samples.
- **Web services API and manual submission** enables any product or malware analyst to submit suspicious samples. Shares new indicators of compromise (IoC) detection intelligence automatically with Trend Micro and third-party products.
- Support for Windows, Mac, and Android™ operating systems.

Source: “Deep Discovery Analyzer” Datasheet,

[www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab](http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab)

### Threat Types

This widget shows the type, amount, and risk level of threats detected in all submissions during the specified time period.

Threat Types				
Period: Last 24 hours ▼		Last refresh: 22/06/2016 14:10:17		
Threat Type	High Risk	Medium Risk	Low Risk	Total
Ransomware	4	0	0	4
Coin Miner	0	0	0	0
Dropper	62	0	117	179
Worm	35	0	0	35
Backdoor	26	0	69	97
Bot	13	0	0	13
Keylogger	5	0	0	5
Downloader	3	0	0	3
File Infector	0	0	0	0
Exploit	0	0	0	0
Rootkit	0	0	0	0

The default period is **Last 24 hours**. Change the period according to your preference.

Click a number under **High Risk**, **Medium Risk**, **Low Risk**, or **Total** to go to the **Submissions** screen and view detailed information.

Source: “Threat Types,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 3, page 9

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

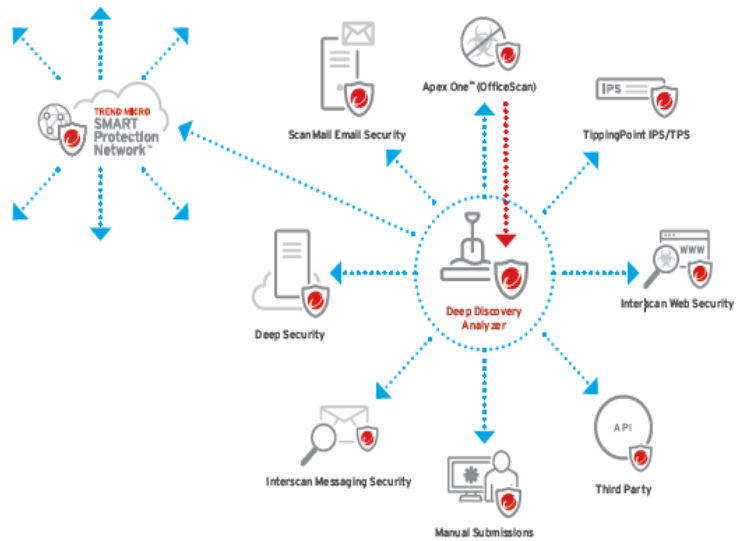
### Smart Feedback Tab

Deep Discovery Analyzer integrates the new Trend Micro Feedback Engine. This engine sends threat information to the Trend Micro Smart Protection Network, which allows Trend Micro to identify and protect against new threats. Participation in Smart Feedback authorizes Trend Micro to collect certain information from your network, which is kept in strict confidence.

Information collected by Smart Feedback:

- Product ID and version
- URLs suspected to be fraudulent or possible sources of threats
- Metadata of detected files (file type, file size, SHA-1 hash value, and SHA-1 hash value of parent file)
- Detection logs (from Advanced Threat Scan Engine, Predictive Machine Learning engine, and Virtual Analyzer)
- Sample of the following detected file types: bat, class, cmd, dll, exe, htm, html, jar, js, lnk, macho, mov, ps1, svg, swf, udl, vbe, vbs, wsf
- Macros in Microsoft Office files

Source: “Smart Feedback Tab,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 4, page 75




- .....▶ Potential threat submissions by any product, in this case Trend Micro™ Apex One™ (Trend Micro™ OfficeScan™) are sent to Deep Discovery Analyzer for further investigation.
- .....▶ If the submission is determined malicious, the verified threat information is sent not only to the submitting product but also to the rest of the security ecosystem for layered protection. Threat intelligence is also sent to the Trend Micro™ Smart Protection Network™ so users around the world can be protected from the once unknown threat.

Source: “Layered Security for Detection and Response” brief, [www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f](http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3b-prd-img-solution-brief-1d3c9f)

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

<p>simulating operating conditions of the protected system in the dynamic decoy system; and</p>	<p>Trend Micro’s accused methods embody simulating operating conditions of the protected system in the dynamic decoy system. Reasonable discovery will confirm this interpretation.</p> <p>For example, Trend Micro’s Deep Discovery Analyzer customizable sandbox (e.g., dynamic decoy system) provides a wide range of capabilities to simulate the operating conditions of the protected system.</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>Custom Sandboxing</b></p> <p style="border: 2px solid red; padding: 2px;">Deep Discovery Analyzer performs sandbox simulation and analysis in environments that match the desktop software configurations attackers expect in your environment and ensures optimal detection with low false-positive rates.</p>  <p style="text-align: right;">1-5</p> </div> <p>Source: <a href="https://docs.trendmicro.com/all/ent/ddan/v6.8/en-us/ddan_6.8_ag.pdf">https://docs.trendmicro.com/all/ent/ddan/v6.8/en-us/ddan_6.8_ag.pdf</a> (emphasis added)</p> <div style="border: 1px solid black; padding: 10px; margin-top: 10px;"> <p><b>Custom sandboxing</b></p> <p style="border: 2px solid red; padding: 2px;">Custom sandboxes use virtual images to match your operating system applications, configurations, and patches. Difficult for hackers to evade, they include a “safe live mode” to analyze multi-stage downloads, URLs, C&amp;C, and more. Sandboxing can be used as further sandboxing capacity for other Deep Discovery appliances or as a scalable stand-alone sandbox. Manual submission allows administrators to investigate suspicious objects.</p> </div> <p>Source: “Custom Sandboxing” Tab, <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analzyer.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analzyer.html</a> (emphasis added)</p>
---	--

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

	<div data-bbox="553 373 672 583"> </div> <p><b>Advanced Detection Methods</b> such as static analysis, heuristic analysis, behavior analysis, web reputation, and file reputation ensure threats are discovered quickly. Analyzer also detects multi-stage malicious files, outbound connections, and repeated C&amp;C from suspicious files.</p> <ul style="list-style-type: none"> <li>• <b>Broad file analysis range</b> examines a wide range of Windows executables, Microsoft® Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing. Custom policies can be defined by file type.</li> <li>• <b>Document exploit detection</b> discovers malware and exploits delivered in common document formats by using specialized detection and sandboxing.</li> <li>• <b>URL analysis</b> Performs sandbox analysis of URLs contained in emails or manually submitted samples.</li> <li>• <b>Web services API and manual submission</b> enables any product or malware analyst to submit suspicious samples. Shares new indicators of compromise (IoC) detection intelligence automatically with Trend Micro and third-party products.</li> <li>• Support for Windows, Mac, and Android™ operating systems.</li> </ul> <p>Source: “Deep Discovery Analyzer” Datasheet,  <a href="http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab">www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html?modal=s3a-prd-img-datasheet-679bab</a></p>
<p>monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code,</p>	<p>Trend Micro’s accused methods embody monitoring sensors in the dynamic decoy system for at least one of actions or results of the one or more portions of code. Reasonable discovery will confirm this interpretation.</p> <p>On information and belief, and for example, Trend Micro’s Deep Discovery Analyzer contains at least one or more sensors capable of analyzing the potential threats (<i>e.g.</i>, actions or results of the one or more portions of code) to the protected system. Trend Micro’s Deep Discovery method analyzes relevant, potentially malicious data, and sends relevant analyses and reports to relevant systems and users. Such detection requires sensors.</p> <div data-bbox="544 1409 1377 1816"> </div> <p>Source: “Detect threats faster with advanced sharing,”  <a href="http://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/deep-discovery-threat-intelligence-network-analytics.html?modal=s5a-prd-img-deep-discovery-445d38">www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/deep-discovery-threat-intelligence-network-analytics.html?modal=s5a-prd-img-deep-discovery-445d38</a></p>



U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

“Organizations are increasingly becoming victims of targeted ransomware when advanced malware gets around traditional security, encrypts data, and demands payment to release the data. Deep Discovery Analyzer uses known and unknown patterns and reputation analysis to **detect** the latest ransomware attacks, including WannaCry. The customized sandbox **detects** mass file modifications, encryption behavior, and modifications to backup and restore processes.”

Source: [https://www.trendmicro.com/en\\_th/business/products/network/advanced-threat-protection/analyzer.html](https://www.trendmicro.com/en_th/business/products/network/advanced-threat-protection/analyzer.html)

Trend Micro’s Custom Sandbox Analysis (e.g., dynamic decoy machine) includes “safe external access to **identify** and **analyze** . . .”



**Custom Sandbox Analysis** uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Source: “Deep Discovery Analyzer,”

[https://www.trendmicro.com/en\\_us/business/products/network/advanced-threat-protection/analyzer.html](https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html).

**Risk Level**

Virtual Analyzer performs static analysis and behavior simulation to identify a sample’s characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings.

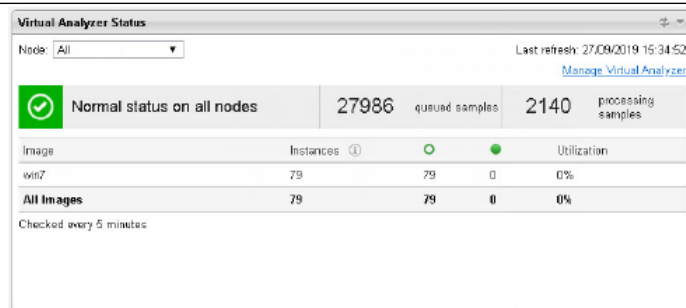
- **Red icon (⊗):** High risk. The object exhibited highly suspicious characteristics that are commonly associated with malware.  
 Examples:
  - Malware signatures; known exploit code
  - Disabling of security software agents
  - Connection to malicious network destinations
  - Self-replication; infection of other files
  - Dropping or downloading of executable files by documents
- **Yellow icon (⚠):** Low risk. The object exhibited mildly suspicious characteristics that are most likely benign.
- **Green icon (✓):** No risk. The object did not exhibit suspicious characteristics.

Source: “Submissions,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 4, page 6

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive



Click **Manage Virtual Analyzer** to go to the **Sandbox Management** screen. For details, see [Sandbox Management on page 4-48](#).

**Normal status on all nodes** indicates all nodes are operating without errors.

If the status shows an error on one or more nodes, go to **Administration > System Settings** and click the **Cluster** tab to view detailed information about the error.

Source: “Virtual Analyzer Status,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 3, page 14

### Threat Types

This widget shows the type, amount, and risk level of threats detected in all submissions during the specified time period.

The screenshot shows the 'Threat Types' window. At the top, it says 'Period: Last 24 hours' and 'Last refresh: 22/06/2018 14:10:17'. Below this is a table with columns: Threat Type, High Risk, Medium Risk, Low Risk, and Total. The table lists various threat types with their corresponding counts. The counts are underlined and blue, indicating they are clickable links. The threat types listed are: Ransomware, Coin Miner, Dropper, Worm, Backdoor, Bot, Keylogger, Downloader, File infector, Exploit, and Rootkit.

Threat Type	High Risk	Medium Risk	Low Risk	Total
Ransomware	<a href="#">4</a>	0	0	<a href="#">4</a>
Coin Miner	0	0	0	0
Dropper	<a href="#">62</a>	0	<a href="#">117</a>	<a href="#">179</a>
Worm	<a href="#">35</a>	0	0	<a href="#">35</a>
Backdoor	<a href="#">26</a>	0	<a href="#">69</a>	<a href="#">97</a>
Bot	<a href="#">13</a>	0	0	<a href="#">13</a>
Keylogger	<a href="#">5</a>	0	0	<a href="#">5</a>
Downloader	<a href="#">3</a>	0	0	<a href="#">3</a>
File infector	0	0	0	0
Exploit	0	0	0	0
Rootkit	0	0	0	0

The default period is **Last 24 hours**. Change the period according to your preference.


Click a number under **High Risk**, **Medium Risk**, **Low Risk**, or **Total** to go to the **Submissions** screen and view detailed information.

Source: “Threat Types,” [https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan\\_6.9\\_ag.pdf](https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf) at Chapter 3, page 9

U.S. Patent 7,010,698  
 “Systems and Methods for Creating a Code Inspection System”  
 Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

	<p><b>Triggered Alerts Tab</b></p> <p>The <b>Triggered Alerts</b> tab, in <b>Alerts / Reports &gt; Alerts</b>, shows all alert notifications generated by Deep Discovery Analyzer. Alert notifications provide immediate intelligence about the state of Deep Discovery Analyzer.</p> <p>The following columns show information about alert notifications created by Deep Discovery Analyzer:</p> <p><b>TABLE 5-1. Triggered Alerts Columns</b></p> <table border="1"> <thead> <tr> <th>COLUMN NAME</th><th>INFORMATION</th></tr> </thead> <tbody> <tr> <td>Triggered</td><td>Date and Time Deep Discovery Analyzer triggered the alert notification.</td></tr> <tr> <td>Level</td><td>Level of the triggered alert notification.               <ul style="list-style-type: none"> <li><b>Critical:</b> The event requires immediate attention</li> <li><b>Important:</b> The event requires observation</li> <li><b>Informational:</b> The event requires limited observation</li> </ul> </td></tr> <tr> <td>Rule</td><td>Rule that triggered the alert notification.</td></tr> <tr> <td>Affected Appliance</td><td>Host name, IPv4 and IPv6 addresses of the appliance affected by the alert notification content, if applicable.</td></tr> <tr> <td>Details</td><td>Click the icon to view the full alert notification details, including the list of notification recipients, subject, and message of the alert notification.</td></tr> </tbody> </table> <p>Source: “Alert Notifications,” <a href="https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf">https://docs.trendmicro.com/all/ent/ddan/v6.9/en-us/ddan_6.9_ag.pdf</a> at Chapter 5, page 2</p>	COLUMN NAME	INFORMATION	Triggered	Date and Time Deep Discovery Analyzer triggered the alert notification.	Level	Level of the triggered alert notification. <ul style="list-style-type: none"> <li><b>Critical:</b> The event requires immediate attention</li> <li><b>Important:</b> The event requires observation</li> <li><b>Informational:</b> The event requires limited observation</li> </ul>	Rule	Rule that triggered the alert notification.	Affected Appliance	Host name, IPv4 and IPv6 addresses of the appliance affected by the alert notification content, if applicable.	Details	Click the icon to view the full alert notification details, including the list of notification recipients, subject, and message of the alert notification.
COLUMN NAME	INFORMATION												
Triggered	Date and Time Deep Discovery Analyzer triggered the alert notification.												
Level	Level of the triggered alert notification. <ul style="list-style-type: none"> <li><b>Critical:</b> The event requires immediate attention</li> <li><b>Important:</b> The event requires observation</li> <li><b>Informational:</b> The event requires limited observation</li> </ul>												
Rule	Rule that triggered the alert notification.												
Affected Appliance	Host name, IPv4 and IPv6 addresses of the appliance affected by the alert notification content, if applicable.												
Details	Click the icon to view the full alert notification details, including the list of notification recipients, subject, and message of the alert notification.												
<p>wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system.</p>	<p>Trend Micro’s accused methods embody monitoring sensors, per the preceding step, wherein the relevant portions of the protected system allow the one or more portions of code to be analyzed in the dynamic decoy system as if the dynamic decoy system were the protected system. Reasonable discovery will confirm this interpretation.</p> <p>For example, Trend Micro’s accused methods include custom sandboxes (e.g., dynamic decoy system) that use virtual images to “precisely match [a user’s] system configurations, drivers, installed applications, and language versions” (e.g., protected system).</p> <div data-bbox="548 1514 1459 1686">  <p><b>Custom Sandbox Analysis</b> uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&amp;C), and more, as well as supporting manual or automated file and URL submission.</p> </div> <p>Source: “Deep Discovery Analyzer,” <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analyzer.html</a>.</p>												

U.S. Patent 7,010,698  
“Systems and Methods for Creating a Code Inspection System”  
Pre-Discovery Evidence of Use for Infringement

Priority Date: February 14, 2001

Note: Statements made herein are illustrative and not exhaustive

	<p>For example, in a video titled “Suspicious Objects,” Trend Micro states: “analyzed in a secure custom sandbox to see what the object would do in your environment” 1:01-1:05. <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection.html</a></p> <p>For example, in a video titled “Detect lateral movement of known, unknown, and undisclosed threats,” Trend Micro states: “secure custom sandbox that mimics your own corporate image down to the OS, application, version, and patches” 1:12-1:20. <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection.html</a></p> <div><h3>Custom sandboxing</h3><p>Custom sandboxes use virtual images to match your operating system applications, configurations, and patches. Difficult for hackers to evade, they include a “safe live mode” to analyze multi-stage downloads, URLs, C&amp;C, and more. Sandboxing can be used as further sandboxing capacity for other Deep Discovery appliances or as a scalable stand-alone sandbox. Manual submission allows administrators to investigate suspicious objects.</p></div> <p>Source: “Custom Sandboxing” Tab, <a href="https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analzyer.html">https://www.trendmicro.com/en_us/business/products/network/advanced-threat-protection/analzyer.html</a> (emphasis added)</p>